

Totemo TrustMail®

Secure Messaging Gateway

Securing Your Data in Motion

INHALT

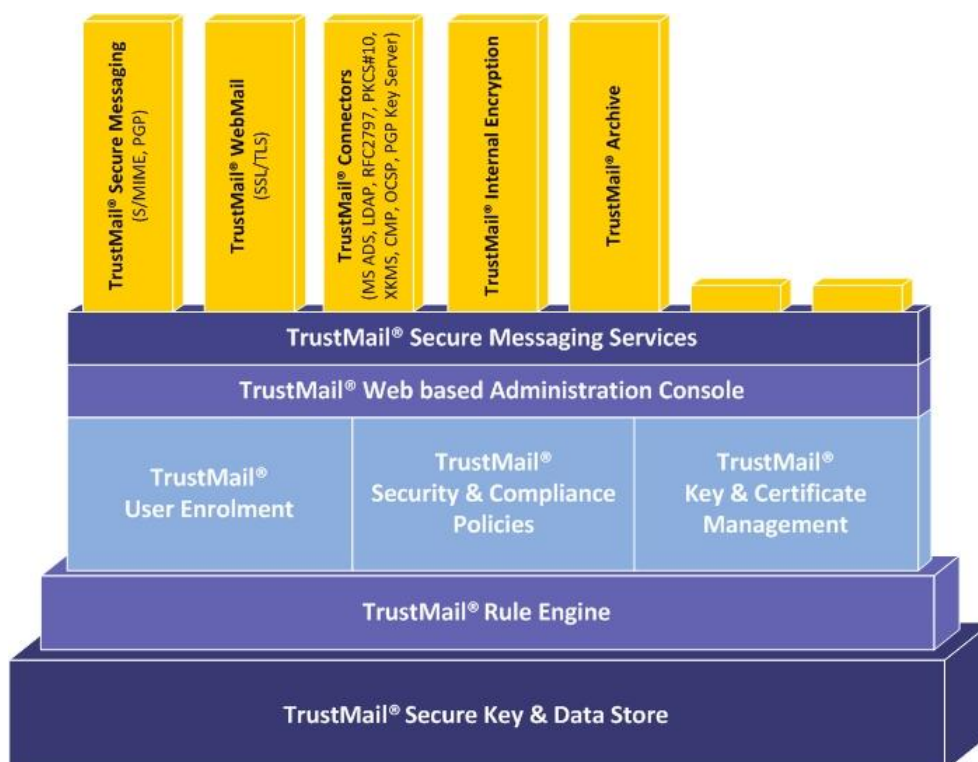
_ Totemo TrustMail® – Securing Your Data in Motion	4
_ Totemo TrustMail® Komponentenmodell.....	4
:: TrustMail®Secure Messaging Gateway.....	4
:: Anti-Spam	5
:: Security Policy und Key Management	5
:: Security Policies	5
:: Key Management	5
:: Totemo TrustMail® Administration Console	7
:: Totemo TrustMail® Rule Designer	8
:: Totemo TrustMail® WebMail	9
_ User Administration	10
:: Registrierung von externen Kommunikationspartnern	10
:: 1. Antwort durch digitale Signierung der Notifizierung	10
:: 2. Certificate Request.....	10
:: 3. Zugriff auf WebMail-Applikation über SSL-geschützte Verbindung.....	10
:: 4. <i>PushedPDF</i>	10
:: Registrierung von internen Benutzern	11
_ Totemo TrustMail® Internal Encryption.....	12
:: De Facto End-to-End-Verschlüsselung mit externen Empfängern	12
:: Die Vorteile gegenüber der klassischen End-to-End-Verschlüsselung	13
:: Internal Encryption – Integration mit BlackBerry® Endgeräten	13
_ Totemo TrustMail® Archive.....	14
_ Warum Sie sich für Totemo TrustMail® entscheiden sollten	15
:: Wer sind wir?.....	16
:: Haben Sie noch Fragen?	16

TOTEMO TRUSTMAIL® - SECURING YOUR DATA IN MOTION

Totemo TrustMail ist eine der innovativsten und erfolgreichsten Secure Messaging-Lösungen, welche die sichere E-Mail-Kommunikation mit internen und externen Kommunikationspartnern sicherstellt. Dieses Standardprodukt wird von sehr namhaften Unternehmen und Behörden zum Schutz vertraulicher E-Mails eingesetzt.

TrustMail ist ein vollständig transparentes System und bietet eine sehr einfache, schnelle und effiziente Einbindung in jede bestehende Mail Infrastruktur wie beispielsweise Microsoft Exchange, Lotus Domino, Oracle Collaboration Suite, GroupWise etc.

Die internen Anwender wie auch die externen Kommunikationspartner müssen keine speziellen Mail Clients oder Client Komponenten installieren, da TrustMail auch mit allen gängigen Mail Clients wie beispielsweise Outlook, Outlook Express, Lotus Notes etc. direkt kommunizieren kann.



Die Registrierung der internen und externen Kommunikationspartner erfolgt vollständig automatisch durch TrustMail. Somit werden die internen Betriebskosten wie auch der administrative Aufwand auf ein absolutes Minimum reduziert. Über die integrierten Schnittstellen kann TrustMail auch mit bereits vorhandenen Verzeichnissen wie LDAP oder MS-ADS sowie auch mit externen PKI Systemen verbunden werden.

Totemo TrustMail stellt sicher, dass

- sämtliche E-Mails mittels S/MIME, PGP oder SSL sicher übermittelt (Secure Transmission),
- der jeweilige Absender identifiziert (Sender Identification),
- die Übermittlung bestätigt (Delivery Confirmation),
- die nicht-Widerrufbarkeit der Nachricht gewährleistet (Non-repudiation) und
- der Nachrichteninhalt geschützt (Content Integrity)

werden können.

Nebst diesen Funktionen beinhaltet TrustMail auch ein umfassendes Policy und Key Management, mit dem auf sehr einfache Art und Weise unternehmensweit gültige E-Mail Security und Certificate Policies definiert werden können.

TOTEMO TRUSTMAIL® KOMPONENTENMODELL

Die Produktarchitektur von TrustMail basiert auf einem eigenen Komponentenmodell und setzt sich aus den Modulen

- TrustMail® Secure Messaging Gateway,
- TrustMail® WebMail,
- TrustMail® Internal Encryption (optionales Modul) und
- TrustMail® Archive (optionales Modul)

zusammen.

TrustMail ist in zwei verschiedenen Produktversionen verfügbar:

- **Totemo TrustMail® Enterprise Edition** bietet den vollen Funktionsumfang, d.h. sie beinhaltet u. a. auch die CA-Funktionalität für externe Kommunikationspartner. Diese Produktversion richtet sich an Unternehmen, die eine zentrale, regelbasierte, vollskalierbare, transparente und vollautomatisierte Secure Messaging Lösung mit PKI-Funktionalität wünschen.
- **Totemo TrustMail® Professional Edition** ist vom Funktionsumfang praktisch mit der Enterprise Edition identisch, wird jedoch ohne CA-Funktionalität für die externen Kommunikationspartner ausgeliefert. Sie richtet sich an Unternehmen, welche eine zentrale, regelbasierte, vollskalierbare, flexible und transparente Secure Messaging-Lösung suchen.

Beide Produktversionen basieren auf derselben innovativen und robusten Software-Architektur, arbeiten nach etablierten Standards und zeichnen sich durch transparente Bedienung und hohe Kosteneffizienz aus.

TRUSTMAIL® SECURE MESSAGING GATEWAY

Mit dem TrustMail Gateway werden sämtliche elektronischen Nachrichten mittels S/MIME oder PGP an zentraler Stelle ver- bzw. entschlüsselt sowie die definierten Security und Certificate Policies umgesetzt. Dadurch steigt die realisierte Sicherheit, da mögliche Flüchtigkeitsfehler und Unachtsamkeiten beim Versenden von vertraulichen Nachrichten praktisch vollständig eliminiert werden.

Der TrustMail Gateway ist ein vollständig transparentes System, das keine Änderung der Arbeitsabläufe für die Kommunikationsteilnehmer voraussetzt. Dadurch kann TrustMail ganz einfach und kosteneffizient auch in bereits existierende Mail-Infrastrukturen eingesetzt werden.

Sämtliche Anwender werden vom TrustMail Gateway automatisch registriert und in einer verschlüsselten Datenbank oder in einem Verzeichnisdienst wie MS-ADS oder LDAP gespeichert. Für jeden registrierten Anwender werden auch seine Credentials wie das von ihm bevorzugte Verschlüsselungsverfahren (S/MIME, PGP, SSL) und alle von ihm verwendeten Public Keys gespeichert.

Sobald ein interner Mitarbeiter eine Nachricht an einen externen Empfänger versendet, werden die gespeicherten Credentials des Empfängers vom TrustMail Gateway überprüft. Ist der Empfänger bereits registriert, wird die Nachricht mit dem entsprechenden Public Key oder digitalen Zertifikat verschlüsselt bzw. signiert. Für den Fall, dass der Empfänger keinen Public Key oder kein digitales Zertifikat besitzt, erhält er von TrustMail automatisch eine Notifizierung mit der Aufforderung, seine Nachricht in der durch eine SSL-Verbindung geschützten WebMail-Applikation abzuholen.

Handelt es sich um einen neuen Empfänger, findet ebenfalls vollautomatisiert eine einfache Enrolment-Prozedur zwischen dem TrustMail Gateway und dem neuen Empfänger statt: Die ursprüngliche Nachricht wird von TrustMail zurückbehalten und verschlüsselt in der Datenbank zwischengespeichert. An deren Stelle wird eine digital signierte Notifizierung übermittelt mit dem Hinweis, dass der Absender eine sichere Nachricht übermitteln möchte, jedoch der Empfänger noch nicht als „sicher“ registriert ist. Mit der Notifizierung bietet TrustMail dem Empfänger drei verschiedene Optionen, wie er seine Nachricht sicher empfangen bzw. lesen kann.

ANTI-SPAM

TrustMail verfügt über eine integrierte Anti-Spam Funktion, mit der die Kopfdaten von E-Mails auf Spam-Inhalte überprüft werden können, bevor sie in das Netzwerk des Unternehmens gelangen. TrustMail unterstützt die Online Abfrage von Blacklists, NES Header Fields Check, Early Spam Relay Connection Interruption und DKIM (DomainKeys Identified Mail).

SECURITY POLICY UND KEY MANAGEMENT

TrustMail beinhaltet ein umfassendes Policy und Key Management, mit dem auf sehr einfache Art und Weise unternehmensweit gültige Security und Certificate Policies definiert werden können.

SECURITY POLICIES

Die Security Policies können auf der Basis sämtlicher Mail Attribute wie beispielsweise Empfänger- und Absenderadresse, Betreffzeile, Nachrichteninhalte, Nachrichteneinstellung, Attachments etc. definiert werden. Dadurch können die Regeln zu den Security Policies so abgebildet werden, dass beispielsweise generell jedes E-Mail an eine bestimmte Domäne verschlüsselt werden muss (Site-to-Site-Encryption), oder, dass die Nachrichten nur dann verschlüsselt werden sollen, wenn die entsprechende Nachrichteneinstellung des Mail Clients die Verschlüsselung impliziert. Die Möglichkeiten zu solchen Regeln sind in TrustMail praktisch unbegrenzt und können auch beliebig kombiniert werden.

In Kombination mit dem integrierten Group Management können sogar E-Mail-spezifische Business Prozesse wie Funktionale Mailboxen, Eskalationsprozeduren, Vier Augen-Prinzip etc. sehr einfach abgebildet und umgesetzt werden.

Wenn für gewisse E-Mails und / oder in Abhängigkeit von bestimmten Geschäftsprozessen eine echte Empfangs- resp. Lesebestätigung benötigt wird, kann TrustMail die Benutzung des WebMail auch für Empfänger mit gültigen digitalen Zertifikaten und Schlüsseln erzwingen.

Die Definition der Security Policies und der damit verbundenen E-Mail-Workflows werden vollumfänglich durch eine eigene grafische Anwenderoberfläche, dem Rule Designer, unterstützt.

KEY MANAGEMENT

Eine weitere wichtige Komponente von TrustMail ist die automatisierte Zertifikats- und Schlüsselverwaltung. Mit der automatischen Registrierung (Enrolment) der Anwender kann das Key Management die schon vorhandenen Zertifikate und Schlüssel selbständig einsammeln und im internen, verschlüsselten KeyStore speichern.

Die TrustMail Administration Console bietet umfassende Einstellungsmöglichkeiten, mit denen die gewünschten Certificate Policies definiert werden können. So ist es beispielsweise möglich, die vertrauenswürdigen Certificate Authorities, die Online-Validierung von Zertifikaten via CRL / ARL und OCSP, die gewünschten Attribute für die Überprüfung der vertrauenswürdigen Zertifikate und Schlüssel, die Gültigkeitsdauer von selber ausgestellten Zertifikaten etc. zu definieren.

Für die internen Mitarbeiter wird automatisch eine Key History geführt, so dass sämtliche E-Mails zu jeder Zeit wieder rekonstruiert werden können, selbst dann, wenn der Mitarbeiter nicht mehr für das Unternehmen arbeitet. Die Key History ist speziell für interne Revisionen aber auch für die Archivierung von E-Mails von zentraler Bedeutung.

TrustMail bietet über die „Dual Keying“ Funktion die Möglichkeit, dass für die internen Anwender mehrere, unterschiedliche Schlüsselpaare verwendet werden können, um beispielsweise die Nachrichten jeweils mit einem S/MIME-Zertifikat bzw. PGP-Schlüssel ab Client zu signieren und mit einem anderen S/MIME- bzw. PGP-Schlüssel auf dem Gateway zu verschlüsseln.

Über die integrierte PKI Komponente von TrustMail können eigene Zertifikate sowohl für die internen Mitarbeiter als auch für die externen Kommunikationspartner automatisch generiert, verteilt und verwaltet werden. Dies ermöglicht die weitgehend automatisierte, schnelle und effiziente Einbindung aller Kommunikationsteilnehmer.

Mit den integrierten Schnittstellen kann TrustMail auch mit einer externen PKI Lösung wie beispielsweise Entrust, Microsoft Certificate Services etc. oder mit einer externen Certificate Authority (CA) wie beispielsweise TC TrustCenter, Swisscom, GlobalSign, S-Trust, SwissSign, VeriSign etc. verbunden werden. TrustMail unterstützt sowohl den PKCS#10 Certificate Request, RFC2797, XMKS als auch CMP. Die Verbindung zur Entrust PKI kann zusätzlich über das Entrust Java Toolkit auf der Basis von SSL, PKIX oder PKCS erfolgen.

TOTEMO TRUSTMAIL® ADMINISTRATION CONSOLE

TrustMail beinhaltet ein umfassendes Policy und Key Management, mit dem auf sehr einfache Art und Weise unternehmensweit gültige Security und Certificate Policies definiert werden können.

Sämtliche TrustMail Komponenten können über ein Web-basiertes Administrationstool verwaltet und an die eigenen Bedürfnisse angepasst werden. Dem Administrator stehen nebst einem Dashboard und dem Message Tracking Center weitere, sehr umfangreiche Möglichkeiten zur Verfügung, mit denen

- die internen und externen Benutzer,
- die Security und Certificate Policies,
- die TrustMail-Notifizierungen,
- Einträge im Group Management und globalen Adressbuch sowie die
- die im TrustMail Archive gespeicherten E-Mails

administriert werden können. Weiter können systemspezifische Einstellungen für die

- Verwaltung sämtlicher in der WebMail-Applikation gespeicherten E-Mails,
- System Agents,
- Log- und Tracking-Funktionen und
- Mail Queues

konfiguriert und verwaltet werden. Die Administration und Konfiguration von TrustMail kann über das integrierte Rights Management auf verschiedene Mitarbeiter im Unternehmen verteilt werden.

Falls TrustMail in einer verteilten oder Cluster Konfiguration installiert und betrieben wird, können sämtliche Einstellungen auf einem einzelnen System vorgenommen und per Knopfdruck auf die anderen Systeme propagiert werden (Single Point of Configuration).

Die Administration Console wird ganz einfach über den Microsoft Internet Explorer bedient.

The screenshot displays the Totemo TrustMail Administration Console interface. It is divided into several sections:

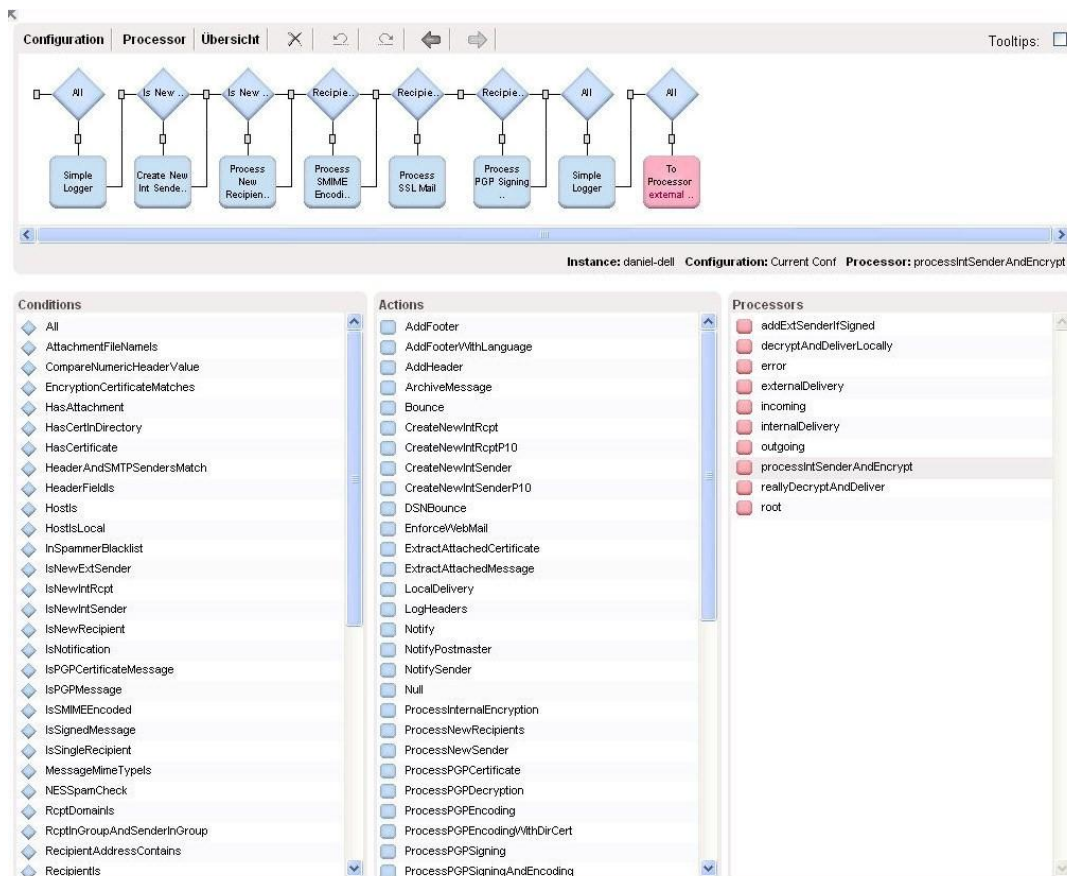
- Nachrichten Übersicht:** Shows email statistics for the last month, including incoming (20358) and outgoing (1202) emails, and error counts.
- Gesicherte Eingehende Nachrichten:** Displays a breakdown of incoming secured messages by format (S/MIME, PGP, WebMail, PDF) and encryption status (signed, encrypted, or both).
- Gesicherte Ausgehende Nachrichten:** Shows outgoing secured message statistics, similar to the incoming section.
- Benutzer Informationen:** A table listing various user types and their counts, such as internal users, disabled users, and license holders.
- Zertifikat Information:** A table showing the distribution of certificates, including S/MIME, PGP, and domain certificates.
- Agenten:** A table listing system agents with columns for Agent Name, Description, Last Run, Type, and On/Off status.

TOTEMO TRUSTMAIL® RULE DESIGNER

Der Rule Designer ist eine auf der Ajax-Technologie basierte grafische Benutzeroberfläche (GUI), mit der die unternehmensweit gültigen Security Policies definiert werden können. Dieses umfangreiche Tool bietet eine „easy to use“ Schnittstelle und wird über einen herkömmlichen Microsoft Internet Explorer bedient.

Die einzelnen Regeln und Attribute zu den E-Mail-Workflows können mit Hilfe von vordefinierten Symbolen sehr einfach definiert und jederzeit wieder an neue Bedürfnisse angepasst werden. Muss beispielsweise eine bestehende Security Policy mit einer zusätzlichen Bedingung erweitert werden, kann diese mittels Drag & Drop aus der Liste der verfügbaren Conditions in die gewünschte Stelle des Workflows integriert werden.

Mit dem Rule Designer entfällt das Erlernen einer proprietären Script- oder Programmiersprache vollständig, was gleichzeitig sowohl die Effizienz als auch den Bedienungskomfort für die Definition der Security Policies erhöht. Die integrierte Java API erlaubt die einfache Anpassung und Erweiterung der standardmässig vorhandenen Bedingungen sowie Aktionen und erlaubt sogar das Einbinden von Business Applikationen wie CRM Systeme etc.



TOTEMO TRUSTMAIL® WEBMAIL

Das TrustMail WebMail ist eine vollständig auf J2EE basierte WebMail-Applikation, mit der alle Anwender über eine SSL-geschützte Verbindung mit dem TrustMail Gateway kommunizieren können. Das TrustMail WebMail spielt bei der automatischen Registrierung der externen Kommunikationspartner eine zentrale Rolle und dient gleichzeitig als sicheres Kommunikationsmittel all jener Anwender, die keinen S/MIME- oder PGP-fähigen Mail Client besitzen oder auf ihren Desktops keine lokalen Schlüssel und Zertifikate installieren und verwalten möchten.

Die Architektur der WebMail-Applikation wurde speziell so konzipiert, dass sie einfach und sehr schnell an das „Look & Feel“ des Unternehmens angepasst werden kann. Der Aufbau ist mit dem von bekannten WebMail-Portalen wie Yahoo, GMX etc. vergleichbar und bietet somit den Vorteil, dass der Anwender seine E-Mails in einer ihm vertrauten Umgebung lesen, bearbeiten und bei Bedarf als PDF-, EML- oder HTML-Datei auf den lokalen Desktop herunterladen kann.

Das TrustMail WebMail beinhaltet standardmässig eine Anwender-Authentisierung auf der Basis von Anwendername und Passwort. Über die TrustMail Administration Console kann die Authentisierung der Anwender sehr einfach an die Bedürfnisse des Unternehmens angepasst werden. Die WebMail-Applikation kann aber auch in ein bereits bestehendes Authentisierungssystem integriert werden.

USER ADMINISTRATION

TrustMail ist so konzipiert, dass neue Benutzer selbständig erkannt und von TrustMail automatisch registriert werden, d.h. ohne jegliche manuelle Interaktion seitens des Absenders oder eines Administrators (Best-Practice-Prinzip). Dadurch wird der administrative Aufwand so gering wie nur möglich gehalten.

Sobald ein E-Mail an einen Empfänger gesendet wird, überprüft TrustMail zuerst, ob dieser Empfänger bereits registriert ist.

REGISTRIERUNG VON EXTERNEN KOMMUNIKATIONSPARTNERN

Wenn es sich um einen neuen Empfänger handelt, wird die ursprüngliche Nachricht von TrustMail zurückbehalten und verschlüsselt in der Datenbank zwischengespeichert. Gleichzeitig wird eine digital signierte Notifizierung an den Empfänger übermittelt, welche dem Empfänger verschiedene Optionen bietet, wie er die vertrauliche E-Mail empfangen resp. lesen kann:

1. ANTWORT DURCH DIGITALE SIGNIERUNG DER NOTIFIZIERUNG

Indem der Empfänger die erhaltene Notifizierung mit seinem eigenen Zertifikat digital signiert bzw. seinen PGP Public Key als Attachment zurück sendet, wird der mitgelieferte Schlüssel von TrustMail automatisch auf seine Gültigkeit überprüft und anschliessend je nach Konfiguration im internen KeyStore oder in einem externen Verzeichnisdienst gespeichert. Anschliessend werden die ursprüngliche und jede zukünftige Nachricht automatisch mit dem entsprechenden Public Key verschlüsselt und dem registrierten Empfänger jeweils direkt übermittelt.

2. CERTIFICATE REQUEST¹

Verfügt der Empfänger über einen verschlüsselungsfähigen Mail Client wie beispielsweise Microsoft Outlook, Microsoft Outlook Express, Lotus Notes etc., kann er sich über die WebMail Applikation oder von einer mit TrustMail verbundenen PKI ein digitales Zertifikat ausstellen und dieses in seinen Mail Client importieren. Sobald das Zertifikat installiert ist, werden die ursprüngliche und jede zukünftige Nachricht von TrustMail automatisch mit dem erzeugten Public Key verschlüsselt und direkt an seine E-Mail Adresse zugestellt.

3. ZUGRIFF AUF WEBMAIL-APPLIKATION ÜBER SSL-GESCHÜTZTE VERBINDUNG

Durch das Aktivieren des in der Notifizierung enthaltenen dynamischen Links wird der Empfänger über eine SSL-geschützte Verbindung mit der WebMail-Applikation verbunden. Bevor er auf das für ihn gespeicherte E-Mail zugreifen kann, muss er sich vorher in der WebMail-Applikation durch Eingabe seines User-Namens und durch Ändern des Einweg-Passworts registrieren. Sobald er sich registriert hat, kann er seine Nachricht lesen und gegebenenfalls beantworten. Weiter hat der Empfänger auch die Möglichkeit, seine Nachrichten als EML-, PDF- oder HTML-Datei auf seinen Desktop herunter zu laden und lokal zu speichern.

¹ Nur bei Produktversion Totemo TrustMail® Enterprise Edition verfügbar

4. PUSHEDPDF

Alternativ kann der externe Kommunikationspartner die Option *PushedPDF* wählen. Dabei wird die zu schützende E-Mail inklusive aller Anhänge in ein PDF Dokument umgewandelt, mittels frei konfigurierbarem symmetrischen Algorithmus verschlüsselt und schlussendlich als Anhang einer E-Mail dem externen Kommunikationspartner zugestellt. Die einzige Voraussetzung für den Empfang eines solchen Dokuments ist ein herkömmlicher, kostenloser PDF Reader wie z. B. der Acrobat Reader von Adobe. Da sich PDF als De-facto-Standard für den Austausch von Dokumenten über das Internet entwickelt hat, sind die meisten PDF Reader für die unterschiedlichsten Plattformen (wie z.B. Linux, UNIX, MAC, Windows, Windows Mobile, Symbian, BlackBerry etc.) frei erhältlich.

REGISTRIERUNG VON INTERNEN BENUTZERN

TrustMail bietet für die Registrierung der internen Mitarbeiter ebenfalls verschiedene Möglichkeiten. So können die internen Anwender automatisch registriert werden, sobald diese das erste Mal eine sichere Nachricht senden bzw. empfangen. TrustMail kann aber auch mit bestehenden User Management Systemen oder Verzeichnisdiensten wie MS-ADS, LDAP etc. verbunden werden und von dort jeweils die benötigten Informationen beziehen. Somit müssen die internen Anwender nicht manuell in TrustMail erfasst werden, sondern können weiterhin über das bestehende User Management administriert werden.

TOTEMO TRUSTMAIL® INTERNAL ENCRYPTION

Dieses einzigartige Modul erlaubt es, die vertraulichen E-Mails auch innerhalb des Firmennetzwerks zu verschlüsseln, ohne dass dafür ein Client Plug-In oder eine zusätzliche Software Komponente installiert werden muss. Das Internal Encryption Modul, das optional zum TrustMail Gateway oder auch als Stand-alone Lösung eingesetzt werden kann, bietet die Möglichkeit, sämtliche E-Mails durchgängig vom Sender bis zum Empfänger zu verschlüsseln, unabhängig davon, ob die Nachricht End-to-End, End-to-Gateway oder Gateway-to-End verschlüsselt sein muss.

TrustMail Internal Encryption ist revolutionär, weil es eine bekannte Schwachstelle des klassischen Gateway-Konzepts löst; traditionelle Secure E-Mail Gateways ver- und entschlüsseln E-Mails ausschliesslich vom bzw. zum Internet (outbound E-Mails). Jedoch sind die vertraulichen Nachrichten innerhalb des Firmennetzwerks nach wie vor ungeschützt bzw. im Klartext lesbar.

Dieser Umstand konnte bis anhin nur mit der klassischen End-to-End-Verschlüsselung gelöst werden, was wiederum die Verwendung von zusätzlichen Client Software Komponenten, proprietären E-Mail-Protokollen oder verschlüsselten Verbindungen notwendig macht, und gleichzeitig dem Unternehmen die Kontrolle über seine E-Mail-Sicherheit entzieht.

TrustMail Internal Encryption beseitigt nun dieses Problem, ohne dass hierfür auf die bekannten Vorteile des serverbasierten Ansatzes wie beispielsweise zentrale Definition und Umsetzung der Security Policies, zentrale Verwaltung sämtlicher Schlüssel und Zertifikate etc. verzichtet werden muss.

Das Konzept ist einfach und dennoch sehr überzeugend: Für jeden Mitarbeiter im Unternehmen stellt TrustMail über die eigene oder eine externe CA ein X.509-Zertifikat aus, wobei der Public Key jeweils in einem zentralen LDAP- oder MS ADS-Verzeichnis im internen Netzwerk des Unternehmens gespeichert wird. Der dazu gehörende Private Key wird entweder direkt im KeyStore des Mitarbeiter Clients oder – den Vorgaben des neuen schweizerischen Bundesgesetzes über die elektronische Signatur (ZertES) entsprechend – auf einem separaten Token gespeichert und steht ausschliesslich dem Mitarbeiter für das Entschlüsseln und Signieren von E-Mails zur Verfügung.

Die im zentralen Verzeichnisdienst gespeicherten Public Keys der Mitarbeiter können für die Verschlüsselung von internen Mails benutzt werden, ohne dass dadurch die Umleitung des internen Mailverkehrs zu TrustMail notwendig ist.

DE FACTO END-TO-END-VERSCHLÜSSELUNG MIT EXTERNEN EMPFÄNGERN

Für die sichere Kommunikation zu externen Empfängern generiert TrustMail jeweils automatisch ein Pro Forma X.509 Zertifikat, das nur innerhalb des Firmennetzwerks gültig ist. Der öffentliche Schlüssel dieses Pro Forma Zertifikats wird ebenfalls im zentralen Verzeichnisdienst gespeichert und ist somit für jeden Mitarbeiter im Unternehmen verfügbar. Damit kann der interne Absender die vertraulichen Nachrichten bereits von seinem Mail Client aus verschlüsselt versenden.

Sobald die mit dem Pro Forma Zertifikat verschlüsselte Nachricht beim TrustMail Gateway ankommt, wird diese automatisch mit dem zum Zertifikat gehörenden Private Key entschlüsselt und optional auf Viren und unzulässigem Content überprüft. Nach erfolgreicher Prüfung werden das E-Mail und sämtliche Attachments mit dem offiziellen Zertifikat oder PGP Public Key des externen Kommunikationspartners verschlüsselt und an seine E-Mail-Adresse weitergeleitet.

Handelt es sich dabei um einen neuen externen Empfänger, speichert TrustMail das E-Mail temporär in seinen verschlüsselten Data Store und initiiert automatisch den Registrierungsprozess (Enrolment). Die Nachricht bleibt nun solange im Data Store gespeichert, bis TrustMail ein gültiges Zertifikat oder einen PGP Schlüssel vom externen Empfänger erhält. Alternativ kann dieser seine vertraulichen Nachrichten im TrustMail WebMail über eine SSL-geschützte Verbindung lesen und beantworten.

DIE VORTEILE GEGENÜBER DER KLASSISCHEN END-TO-END-VERSCHLÜSSELUNG

- Im Gegensatz zur klassischen End-to-End-Verschlüsselung bleibt die gesamte Administration der Zertifikate und Schlüssel zentral beim TrustMail Gateway.
- Durch die Umschlüsselung auf dem Gateway sind die zentralen Security Checks wie Virenkontrolle, Content Filterung, Anti-Spam etc. nach wie vor gewährleistet.
- Das „Einsammeln“ der Zertifikate und Schlüssel der externen Kommunikationspartner erfolgt automatisch durch TrustMail und muss nicht vom einzelnen Mitarbeiter wahrgenommen werden.
- Funktionale bzw. Shared Mailboxen sind vollumfänglich unterstützt, da TrustMail die Nachrichten für jeden einzelnen Empfänger mit dessen Public Key verschlüsselt.
- Ebenso können weiterhin Delegationen und Stellvertretungsregelungen problemlos umgesetzt werden.
- Verschlüsselte E-Mails sind auch von Mitarbeitern und Systemadministratoren nicht mehr einsehbar.

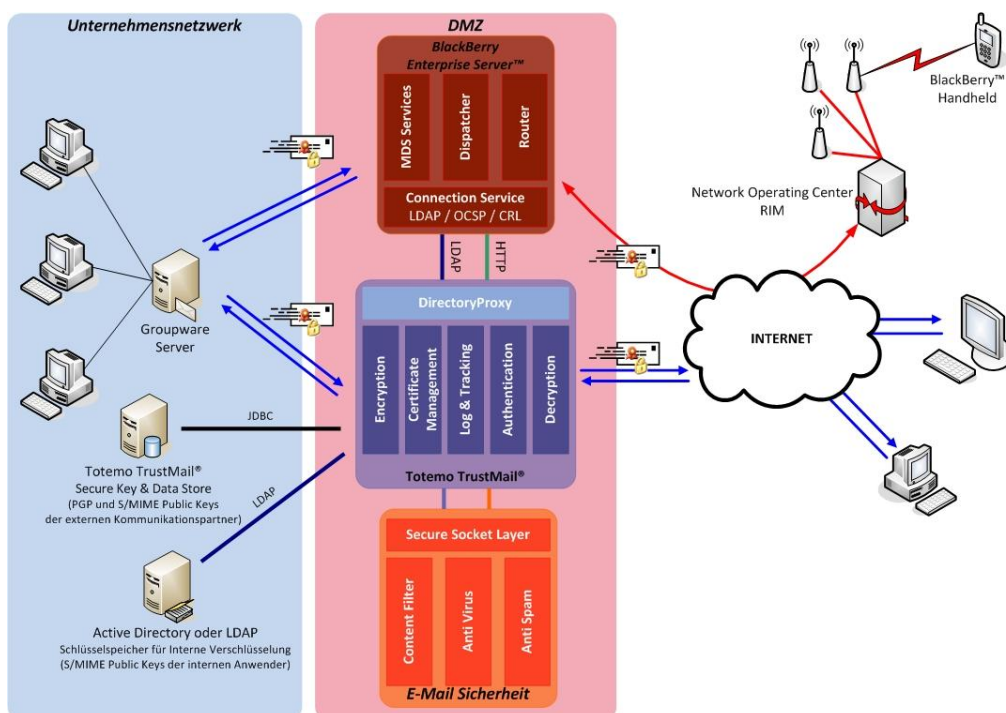
INTERNAL ENCRYPTION® – INTEGRATION MIT BLACKBERRY® ENDGERÄTEN

In Kombination mit dem S/MIME Support Package (SSP) von Research in Motion (RIM) können die E-Mails auch vom Mail Client bis zum BlackBerry® Device und zurück verschlüsselt werden. Dadurch bleiben die Nachrichten auch vor dem Zugriff des BlackBerry® Enterprise Servers™ (BES) vollumfänglich geschützt.

Die Integration von BlackBerry ist ganz einfach und identisch mit der eines internen Mail Clients. Lediglich die beiden folgenden Voraussetzungen müssen auf dem BlackBerry Device erfüllt sein:

- a) Das S/MIME Support Package (SSP) von Research in Motion muss auf dem BlackBerry Device installiert sein, damit die Public Keys der internen und externen Empfänger synchronisiert resp. aus dem zentralen Repository gelesen werden können.
- b) Auf dem BlackBerry Device muss der persönliche Private Key installiert sein, damit die empfangenen Nachrichten entschlüsselt und gelesen werden können.

Sobald diese Voraussetzungen erfüllt sind, können auf den BlackBerry® Devices verschlüsselte und signierte Nachrichten empfangen und versendet werden, und zwar unabhängig davon, ob der Kommunikationspartner ein interner Benutzer (Mitarbeiter) oder ein externer Empfänger ist.



TOTEMO TRUSTMAIL® ARCHIVE

Das TrustMail Archive ermöglicht es, jedes E-Mail – einschliesslich der dazu gehörenden Attachments – sicher zu archivieren, zu verwalten und anschliessend leicht darauf zuzugreifen. Die E-Mails werden in einem zentralen Repository archiviert, der eine langfristige, sichere Ablage und sofortige Verfügbarkeit gewährleistet. Es stellt zudem eine komfortable und kostengünstige Art der E-Mail-Aufbewahrung dar.

TrustMail Archive verwaltet sowohl die Metadaten (Informationen über den Kontext, aus dem die E-Mails und Attachments stammen) als auch den Content selbst. Die Metadaten werden grundsätzlich in einer relationalen Datenbank gespeichert. Dabei können die Metadaten wie Absender, Empfänger, Betreff, Kategorie, Attachment Name sowie Sende- und Archivierungsdatum im TrustMail Archive abgelegt werden, um ein gespeichertes E-Mail exakt und schnell wieder lokalisieren zu können.

Der TrustMail Administrator entscheidet darüber, ob der Content, d.h. das E-Mail und die Attachments, in einer relationalen Datenbank, auf einem File Server, optischen Speichermedien, Magnetbändern oder einem anderen langfristigen Speichermedium abgelegt werden soll. Mit digitalen Signaturen lässt sich auch verhindern, dass das E-Mail unbemerkt verändert wird. Aufgrund der gemeinsamen Systemarchitektur kann das TrustMail Archive auf den TrustMail KeyStore und auf die Key History jedes einzelnen Anwenders zugreifen. Somit wird sichergestellt, dass auch verschlüsselte Nachrichten jederzeit wieder mit dem richtigen Schlüssel entschlüsselt und angezeigt werden können. Sämtliche Attachments werden jeweils mit den originalen Dateiendungen gespeichert und bleiben somit jederzeit ausführbar.

Im Rule Designer des TrustMail Gateways sind standardmässig vordefinierte Archivierungsregeln enthalten, mit denen aufgrund bestimmter Kriterien sowohl ankommende als auch ausgehende E-Mails und die dazu gehörenden Attachments archiviert werden können.

Der Zugriff auf die archivierten E-Mails erfolgt ausschliesslich über die TrustMail Administration Console. Der Administrator vergibt für jeden Anwender die notwendigen Zugriffsrechte, so dass dieser beispielsweise nur auf die ihn betreffenden E-Mails zugreifen kann.

Die Vorteile von TrustMail Archive sind:

- Verbesserte Effizienz und Produktivität
- Verringerte Kosten dank niedrigerem Wartungsaufwand
- Beachtung der rechtlichen Vorschriften und Schutz vor juristischen Risiken

WARUM SIE SICH FÜR TOTEMO TRUSTMAIL® ENTSCHEIDEN SOLLTEN

- Jeder beliebige Empfänger kann von TrustMail sicher erreicht werden, selbst wenn er keinen verschlüsselungsfähigen Mail Client besitzt.
- Sie können mit all Ihren externen Kommunikationspartnern verschlüsselte Nachrichten austauschen, ohne dass diese TrustMail oder ein anderes äquivalentes Produkt installieren müssen. Alle Beteiligten können weiterhin über ihre Mail Clients miteinander kommunizieren.
- TrustMail kann sehr einfach, schnell und effizient in jede bestehende Mail-Infrastruktur integriert werden, in der Regel innerhalb von nur einem Tag.
- TrustMail unterstützt alle bekannten Mail Server wie Microsoft Exchange, Lotus Domino, Oracle Collaboration Suite, GroupWise etc. Ihre bereits getätigten Investitionen sind vollumfänglich geschützt.
- Die einfache und transparente Funktionsweise von TrustMail eliminiert den Schulungsaufwand für alle Anwender und reduziert die Betriebskosten signifikant.
- Weder Ihre internen Mitarbeiter noch Ihre externen Kommunikationspartner müssen dedizierte Mail Clients oder Client Komponenten installieren. Das macht TrustMail sehr kosteneffizient und reduziert die Integrations- und Wartungskosten auf ein absolutes Minimum.
- Der hohe Automatisierungsgrad von TrustMail bietet höchstmöglichen Komfort bei gleichzeitig vollster Flexibilität und höchster Sicherheit.
- Mit den unternehmensweiten Security Policies werden mögliche Flüchtigkeitsfehler und Unachtsamkeiten beim Versenden von vertraulichen Informationen praktisch eliminiert.
- Die automatische Registrierung von internen Mitarbeitern und externen Kommunikationspartner entlastet Ihre täglichen Arbeitsabläufe von unnötigen administrativen Aufgaben.
- Das Einsammeln der Zertifikate und Schlüssel Ihrer externen Kommunikationspartner erfolgt automatisch durch TrustMail. Ihre internen Anwender müssen sich somit nicht um das Zertifikatshandling, CRLs und dergleichen kümmern.
- Auf Wunsch können die Nachrichten sogar innerhalb des Firmennetzwerks verschlüsselt werden. Mit dem optionalen Modul *Internal Encryption* werden die vertraulichen Nachrichten vom Mail Client bis zum Gateway und umgekehrt auf der Basis von S/MIME-Zertifikaten verschlüsselt, ohne dass dafür Plug-Ins oder andere Software Komponenten client-seitig installiert werden müssen. Dies ist gegenüber anderen Secure Messaging Gateway Anbietern ein signifikanter Technologie-Vorsprung.
- Geschäftsrelevante E-Mails können ganz einfach in einem zentralen, verschlüsselten Repository archiviert und verwaltet werden. Mit digitalen Signaturen kann verhindert werden, dass archivierte E-Mails verändert werden.
- TrustMail bietet verschiedene Standardschnittstellen zu Verzeichnissen und Fremdsystemen, was die Einbindung in Ihre bestehende Systemarchitektur erheblich erleichtert, und bietet Ihnen somit den bestmöglichen Freiraum für zukünftige Produktentscheide.
- TrustMail beinhaltet standardmässig die „Dual Keying“ Funktion, mit der die internen Anwender ihre persönlichen Zertifikate bzw. Schlüssel für das Signieren von Nachrichten auf ihren Clients verwenden können.
- TrustMail ist zu hundert Prozent „Made in Switzerland“. Alle Komponenten sind von uns selber entwickelt worden. Das gesamte Produkt Know-how ist vor Ort in Küsnacht vorhanden. Das macht uns zu einem idealen Partner für Ihr Unternehmen.

WER SIND WIR?

Die Totemo AG, ein Schweizer Softwareunternehmen, entwickelt und vertreibt das Produkt Totemo TrustMail®, eine Standardsoftware für die Verschlüsselung von vertraulichen E-Mails (Secure Messaging). TrustMail erlaubt die regelbasierte Ver- und Entschlüsselung von E-Mails und kann ganz einfach in jede bestehende E-Mail-Infrastruktur integriert werden. Das Produkt ist in zwei verschiedenen Versionen erhältlich: TrustMail Enterprise Edition und TrustMail Professional Edition. Beide Produktversionen basieren auf der gleichen innovativen Software-Architektur, arbeiten nach internationalen, etablierten Standards und zeichnen sich durch transparente Bedienung und hohe Kosteneffizienz aus. Zu den Kunden von Totemo zählen namhafte Organisationen und Unternehmen aus den Branchen Financial Services, Government, Application Service Provider (ASP), Health Care, Industrie und Professional Services.

Das Unternehmen wurde im September 2001 gegründet und ist in Küsnacht (ZH) domiziliert.

HABEN SIE NOCH FRAGEN?

Zögern Sie nicht, uns zu kontaktieren:

Totemo AG
Freihofstrasse 22
CH-8700 Küsnacht

phone: +41 (0) 44 914 9900
fax: +41 (0) 44 914 9999
e-mail: info@totemo.ch
website: www.totemo.ch

© Totemo AG